Remarks

This response is to the Office Letter mailed in the above-referenced case on February 29, 2008

Rejection over 35 U.S.C. 103(a)

Claim 38, 40 - 50, and 52 - 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Renwick (US 7,151,775) in view of Comstock (US 6,452,920).

Examiner's rejection

Regarding claims 38 and 50, Renwick teaches:

(a) at a first node in a virtual private network (VPN) / subnetwork (fig. 1 box 22, fig. 3 box Router A, col. 6 lines 32-35) , using a first header portion of a data packet, the first header portion indicating the first node as a source node and a second node in the VPN as a destination node, generating a value associated with the source and destination nodes (fig.3 Router A, router A assigns incoming traffic to one of LSPs using IP header, hash operation include performing division on IP source and destination addresses, Col. 6, lines 33-50). Note the Examiner corresponds the VPN of the applicant with the subnetwork of the reference.

(b) creating a second header portion for the data packet including the value associated with the source and destination nodes (inner label value implicitly carries the IP address hash information calculated at original ingress, col. 9 lines 46-55);

(c) using the second header portion, selecting one of a plurality of possible paths on a the network connected to the VPN for forwarding the packet (fig.3 Router A, router A assigns incoming traffic to one of LSPs using IP header, hash operation include performing division on IP source and destination addresses, col. 8 lines 32 - 58, inner label value implicitly carries the IP address hash information calculated at original ingress, col. 9 lines 46-55).

Although Renwick teaches using the second header portion, selecting one of a plurality of possible paths on a the network connected to the VPN for forwarding the packet, the reference is silent on one of a plurality of possible paths is on a ***second network.*** However, Renwick does teach tunneling (col. 9 lines 46-55). Comstock teaches tunneling between networks (col. 2 lines 35-37).

Therefore it would have been obvious to one of ordinary skill in the art, to modify the system of Renwick by tunneling the hash value between two networks, as suggested by Comstock. This modification would benefit the system by alleviating the router of the responsibility of making the routing decision since the decision was made upstream.

Although the combination teaches the first node, router "A", as the source node of the subnetwork (Renwick: fig. 3), the combination is silent on the first node is the source node. However, this figure is only an illustrative example. If router "A" were the source of the packet, it would have been obvious to one of ordinary skill in the art, to include in the header of the packet the IP address for router "A" as the source IP address. This modification would benefit the system by informing the destination node where the packet originated.

Applicant's response

Applicant points out that the primary reference of Renwick is commonly owned and has a common inventor with the present application. At this time, applicant would rather overcome Renwick with amendments to more particularly point out the distinguishable differences in the Renwick patent from those of the present application. Applicant also gives valid arguments to support applicant's claimed subject matter as being patentable over the patent of Renwick.

Claims 38-50 are herein amended to point out that the second network is the Internet and the source and destination nodes are in the same VPN. The inventors of the present invention solve the problem faced in routing large volumes of packets within the same VPN.

Applicant's background portion points out that one area in which traffic

engineering becomes difficult is in the case of VPNs. In general, VPNs exist in multiple geographic locations. Interconnection of these locations may be done by using public Internet IP service. Because VPNs make use of non-standard protocols and addresses, the addresses used inside a private network may reuse the same address values used in parts of the public Internet. Similarly, multiple different private networks may reuse the same address values. It is not possible to simply transmit the private IP packets over the public Internet, because the use of non-standard addresses will cause the addresses of the packets to be confused. Because of this dynamic VPN packets are typically encapsulated inside IP packets with standard IP source and destination addresses for transmission over the public Internet.

Using this form of encapsulation, packets associated with any particular VPN have a single pair of IP source and destination addresses. The result is that a hash function will always return the same value for any one VPN. This approach does not allow packets from a single VPN to be spread among multiple paths through the communications network. This is a particular problem for very large VPNs having only one routing path available as the routing of data packets becomes degraded.

Applicant's invention, as amended, solves said problem by providing a method and system for transferring a packet of data from a source in a VPN through the Internet back to a destination in the same VPN using multiple communication paths through the Internet. This is especially advantageous in that any VPN packets from a single source and destination in the VPN can be sent over the Internet and a packet from the same VPN having a specific source and destination different from the VPN packet mentioned immediately above, may travel by a different path through the Internet. In this manner routing VPN packets through the Internet become source node and destination node dependent, not VPN dependent, as in the prior art.

Applicant points out that Renwick, as seen in Fig. 1 and 3 includes sub-networks 22 and 122, which can be considered virtual private networks and are positioned between the source and destination nodes. Renwick creates sub-networks in order to route packets from a source and destination in the Internet. In applicant's invention the Internet is

positioned between the source and destination nodes in the VPN. Applicant points out that the tunneling (one path) as taught in Comstock teaches away from the ability to route VPN packets among a plurality of Internet paths back to the same VPN, as claimed.

Applicant believes that claim amendments and arguments given above should serve to adequately overcome the art presented by the Examiner. Therefore, claims 38 and 50, as amended, are patentable over the art of Renwick and Comstock. Claims 39-43, 45-49, 52-55 and 57-61 are patentable on their own merits, or at least as depended from a patentable claim. Claims 44, 51 and 56 are herein canceled.

Summary

The applicant therefore believes that claims 38-61 are patentable over the art, and respectfully request reconsideration, and that the case be passed quickly to issue. If any fees are due beyond fees paid with this amendment, authorization is made to deduct those fees from deposit account 50-0534. If any time extension is needed beyond any extension requested with this amendment, such extension is hereby requested.

Respectfully Submitted,
Ross W. Callon et al.

By */Donald R. Boys/*
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
831-768-1755